



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 01 septembre 2005
N° CERTA-2005-AVI-326

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de DameWare Mini Remote Control

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-326>

Gestion du document

Référence	CERTA-2005-AVI-326
Titre	Vulnérabilité de DameWare Mini Remote Control
Date de la première version	01 septembre 2005
Date de la dernière version	–
Source(s)	Historique des versions du produit DameWare NT Utilities
Pièce(s) jointe(s)	Aucune

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Exécution de code arbitraire à distance.

2 Systèmes affectés

DameWare Mini Remote Control versions 4.8.x et antérieures.

3 Description

DameWare Mini Remote Control est une application client/serveur permettant l'administration à distance de machines sous Windows. Il est inclus dans la suite d'outils DameWare NT Utilities mais peut être installé indépendamment.

Une vulnérabilité de type débordement de mémoire dans le traitement de la variable username permet l'exécution de code arbitraire à distance.

Des outils permettant l'exploitation automatique de cette vulnérabilité sont disponibles sur l'Internet.

4 Contournement provisoire

Filtrer le port 6129/tcp.

5 Solution

Mettre à jour DameWare en version 4.9.x. La dernière version est la 4.9.2.4 (voir section Documentation pour connaître les sites proposant des mises à jour de DameWare).

Note :

Au moment de la rédaction de cet avis, le site <http://www.dameware.com> est indisponible.

6 Documentation

- Site de DameWare :
<http://www.dameware.com>
- Historique des versions de DameWare :
<http://www.dameware.co.uk/history.asp?group=Products>
- Sites alternatifs pour le téléchargement de DameWare :
<http://www.dameware.co.uk/thankyoudownload.asp?group=Downloads>
<http://www.dameware.co.uk/thankyouremote.asp?group=Downloads>
<http://www.dameware.fr>

Gestion détaillée du document

01 septembre 2005 version initiale.